orca security

GSS Galaxy Software Services 叡揚資訊

EBOOK

如何擔任首席資訊安全官

VOLUME 1

前 91 日

安迪·埃利斯（Andy Ellis）

目錄

orca security

GSS Galaxy Software Services 叡揚資訊

orca security
GSS Galaxy Software Services 叡揚資訊

介紹

歡迎來到你的新 CISO 工作！無論你是第一次擔任首席資訊安全官，還是您第十次擔任首席資訊安全官，此文件作為一個快速參考指南。希望它能協助你把所有的事項處理的井然有序，各種流程得心應手。本指南是高層次的說明，包含您應該考慮的領域，盡量避免在特定的技術描述過多細節。

新職務通常會有九十天的試用期（或“蜜月期”），新高階主管必須適應新的環境。在這個期間結束後，你的僱主將預期你正在執行一個安全計劃，你需要見的任何人都已經建立了聯繫，你計劃的任何重大變更都已經啟動。本指南涵蓋了第一季度（精確的說是91天），並介紹了開始一些早期快速成功需要考慮的所有事項。

使用本指南

當你開始你的新職務，試圖運作自己的工作時，你需要同時進行許多平行作業。熟悉新環境不是一個線性過程；你需要同時收集有關人員、企業結構、流程、工具和風險的資訊。本指南將協助你思考要問哪些問題才能熟悉這些領域。每個部分都涵蓋一個入職主題，但實務上你需要同時處理所有主題。

建議你快速通讀整個指南，以瞭解需要同時在哪些領域做什麼事 – 在評估安全架構時，制定正確的計劃並同時與人會面。在任何階段，你都能使用本指南作參考，確保你不會錯過關鍵任務。

ABOUT THE AUTHOR

Andy Ellis 於 2021 年入選 CSO 名人堂，因此他應該對成為 CISO 有所瞭解。他還寫了一本書（1% Leadership，由 Hachette Go 出版），這在建立團隊和企業方面都有一些相關性。他是 ORCA Security 的首席顧問資訊安全官，YL Ventures 的運營合夥人，並擔任其他十幾個兼任職務。

準備開始

由於這系列中還未有第零卷《擔任 CISO 的機會》，本指南將始於你在新角色開始前應該理解的一些事情：了解你剛剛加入的公司。如果你尚未開始，你可以在外部進行很多這方面的研究，提前了解一些情況。請注意，你將會不斷檢驗你的假設並修正。

瞭解您的公司：關鍵問題

每個公司都是不同的。有些公司已經密切監控其員工的內部威脅，當你新提出一系列工具來進一步監控員工行為、實施強大但緩慢的工作流程來保護工作流程或限制可用性以保護敏感資訊時，沒有人會抗議。但是，當你嘗試將這些相同的建議套用於一個更具合議性質的公司時，例如一個將權力分配給員工，你會發現你處處遇到障礙。所以你的第一步是瞭解你的公司。不僅僅是在高層次上，你還需要繪製整個公司的組織圖，並了解不同的事業單位有哪些不同的規範。其中大部分可能與你將要做的工作並行。

本節涵蓋你應該知道的內容，先瞭解公司的狀態來決定自己要採取的姿態，“與人會面”部分介紹了在開示工作後如何收集人事資訊。你可以作為你與同事、利害關係人互動的參考，並作為構建安全架構的輸入。每個部分都涵蓋一個關鍵問題，可協助你區分自己的公司與其他公司。

GOAL — 定義公司的業務以及這些如何限制CISO（首席資訊安全官）的角色和責任。

矽基還是碳基？

當你探索公司的各個部分時，請先尋找公司文化的主導典範：該公司文化是矽基還是碳基。在矽基文化中，人類通常被視為業務的必要零件之一，但主要的管控位於電腦系統中。這類型通常存在於業務規模足夠大，需要將邊際成本降至最低來支持大規模商業的模式。此典範通常側重於盡可能消除人工工作，而安全需求通常以消除內部威脅為導向，例如客服中心多屬於這一類；當你發現操作"系統數據"的比例越高，而越少" 人工介入"，就越是處於矽基公司文化中。在碳基公司文化則相反，人類通常是任何流程的核心。你會發現 IT 流程與使用者之間存在緊張關係：IT 流程認為電腦系統很重要，但其使用者則認為自己比他們使用的IT系統更重要。

在矽基公司中，你應該更加關注於降低可衡量的風險。在碳基公司文化中，你應該重點關注其資安管控的使用者體驗，因為糟糕的使用者體驗會顛覆任何計劃。

投鼠忌器還是孤注一職？

大多數公司都很難闡明他們的風險承受能力，但通常有一種簡單的方法來評估它是接近於零還是無窮大：你是在賠錢（例如新創公司），還是在賺錢（像大多數老牌公司）。如果你正在賺錢，那麼你的操作可能相對保守而顯得投鼠忌器。通常會選擇規避風險，並且避免跳入危險，尤其只為了微不足道的好處。一個成熟的公司可能會因重大失敗而損失慘重，因此往往會行動得更慢，試圖避免犯下明顯的錯誤。另一方面，一家急需下一頓飯而孤注一職的公司總是面臨滅亡的風險。它必須快速行動，冒著高風險，只是為了吃下一頓飯。尤其當你已經註定要滅亡時，大量的風險根本不會威脅到你。

如果你身處一個絕望的公司中，那麼你會遇到快速行動的冒險行為，並抵制施行安全流程，因為這可能會減慢速度，且對使用可能存在缺陷的尖端工具有更大的容忍度。反之，在一個穩定的公司中，你會發現對穩定流程的接受度更高，對不穩定的解決方案的容忍度較低。

公司處於危機中，轉型中還是穩定運作？

有些事情會導致你的公司選擇聘請首席資訊安全官。一般有三種不同的情況。一個是你被帶進來解決危機，通常是在違規之後。也許你是他們的第一位首席資訊安全官，你可以快速的推動任何方案。也許相反，企業已經有一個安全計劃，並且有一個首席資訊安全官，你被帶進來將計劃過渡到不同的成熟度或重點級別。也或許公司的一切都很順利，安全評鑑很正常，你只是進來繼續運行一個偉大的流程。

重要的是你要瞭解公司位在這個光譜上的哪個位置。處於危機中的企業將尋求快速、可操作的技術勝利。一個在過渡中的企業可能希望看到你進行結構性企業變革。一個穩定的企業則不希望聽到你為了新官上任而放三把火燒毀它們。

大鯨魚或小蝦米？

公司（包括你的資訊安全團隊和整個公司）的規模是影響安全計劃的重要因素。一家財富 100 強公司裡會有多個獨立部門，可能只會需要你運作既有管理機制和提供建議；而一家鬥志高昂的新創公司，重點於完成其第一份 SOC 報告。你可能是整個公司團隊的一份子，需要自己部署和運行安全系統；或者你領導一個小組，專注於高效的執行和運營；亦或者你可能正在管理一個大型公司，平衡整個公司的風險。重要的是，不僅要知道你承接的公司規模，還要了解你的利害關係人希望建造的公司類型。

藏樹於林中還是眾人焦點？

某些公司似乎從不引起人們的注意，而某些公司似乎總是出現在新聞中。你未來要如何處理安全問題將受到此影響。雖然只有少部分的商業對手執行的競爭策略是會攻擊任何人，但也有可能因為你有一些有趣的資產，或者你的商業模式有爭議或甚至是喜歡亂說話的高階管理者，讓你的競爭對手攻擊你。了解為什麼人們為什麼會以你為目標，以及他們的具體目標是什麼，可能有助於設計一些特別針對性的防禦措施。

制定廣泛的戰略還是執行區域戰術？

瞭解你的團隊在企業內的位置。如果你坐在高階管理者（例如 CEO）附近，你可能在整個企業中擁有廣泛的治理，能夠制定強勢的（儘管並不總是強制執行）公司政策。相反，你的團隊可能深深埋在於企業內部，而你的任務是簡單地執行戰術安全計劃。也許你兩者兼而有之，你必須同時兼顧你的政策的執行和各層面的戰略措施。

得到狀態意識 (Situational Awareness)

剛到一家公司最困難的部分是你這麼多事情你應該要知道卻所知之甚少。如何學習，而且學得快，將是成功的重要關鍵。你需要向公司內的人學習，同時你要開始更深入地了解公司業務、你所處的環境和各環節的關鍵參與者。

與人會面

在這 91 天的試用期內，你必須認識很多人。每個為你工作的人，你、你的同僚、執行團隊，以及希望有機會能認識董事會成員。雖然你可能因為你的技術技能被錄用，但對你的工作成效的最終評價的方式是人際交往能力和你對流程的理解。

在這些人的會面中，你有幾個目標要達到，他人也會對你有所期望，你需要平衡所有這些期望。你會有一些人對你的加入感到興奮，而有些人則很緊張。你需要引導這種興奮，同時確保你不會被過度期望；你需要緩解這些緊張情緒。你需要向在公司工作了一段時間的人請教，以加速你自己對公司的瞭解。你需要了解公司的文化常用語言，例如「關鍵風險」等術語的定義，瞭解哪些縮寫或文字會引起共鳴，哪些不會。你要避免犯下一些政治錯誤，例如稱讚某些人最近失敗的項目...或者詆毀一些在你上一個企業中沒用，這裡的每個人卻都喜歡的東西。最後，你要設定度過 91 天的 ”蜜月期“ 後的目標。

GOAL — 建立融洽關係，確立信任，並獲取評估安全計劃所需的資訊。

平衡他人對你的期望

人的類型	你應該	但不要
興奮	引導興奮	讓人過度期待
緊張	舒緩緊張	無視擔憂
老鳥	學習歷史與文化	因循苟且
菜鳥	重視靈感與創意	忽略邊際效應

你的團隊

你需要儘快與所有為你工作的人會面，無論是直接還是間接。這應該是你第一週的工作目標，建議召開一次全員會議進行自我介紹，這樣你的新同事就可以開始瞭解你，聽聽你希望他們如何聯繫你，以及與你聯繫什麼。如果有分很多子團隊，參加每個子團隊的會議來自我介紹（這些可能發生在你的第一週之後，但要儘速安排行程）。根據團隊的規模，盡可能個別安排與每個團隊成員進行會議。即使這是一個處於危機中的企業，並且你將做出重大改變，你也需要瞭解現況，同時你必須維持穩定。要注意沒有與新老闆見面很常被解讀成「我們都會被解僱」的信號。

在這些會議期間可能要問的一些重要問題：

- 你的團隊主要負責什麼工作？有哪些我可能不容易察覺但卻是有價值的工作？
- 上一任CISO推動的哪些議題是非常有價值的，我應該確保注意到？
- 相反地，有哪些他們推動的是你覺得無法理解其價值的事物，我應該仔細查看以確定是否可以停止？
- 我們企業中最大的缺口是什麼？如果我們有一個空缺的職位，應該放在哪裡？
- 有哪些我們沒有做但卻總是必須很尷尬的向人解釋我們沒有做的事情？
- 我們至今如何衡量成功？每個人都對這些衡量標準保持一致嗎，還是有一些是利害關係人尚未同意的？

請注意，在所有這些問題中，你要信任從團隊那裡得到的資訊。雖然你應該保持一些懷疑態度——畢竟，人類並不完美——但在你的第一次相遇中，你的目標是傾聽他們願意與你分享的一切。即使你聽到了難以置信的事情，現在也不是解決它們的時候。

同僚

雖然與你的團隊保持穩定很重要，但你的同僚態度通常會決定你的職涯成敗（或至少一部分是）。你與同僚之間的對話最終目標是讓他們成為你的安全計劃的擁護者。最好的方法是讓他們參與你推動的項目。相對於你的團隊來說，對於他們你會有不一樣的問題組。這裡提供兩個最重要的問題組。

這些問題是用來了解你的同僚是神隊友還是豬隊友的隊友候選人清單的重要問題，並有可能為你帶來一些政治資本。你在談話過程應該把這些問題巧妙的編織到你的談話中，而不是逐條盤問。

- 有哪些我們正在做的高成本而低價值， 你認為我們應該停止的安全實踐？
- 有哪些我們沒有做的安全實踐是什麼，你認為我們應該做的？
- 你的團隊如何為公司提供價值？你如何衡量你的團隊的成功？
- 我的團隊能提供什麼協助？我們至今做得如何？
- 安全議題多常出現在你的雷達上？
- 你上次向高階主管團隊進行簡報的狀況？ 我能得到你們投影片的副本嗎？如果你有 Roadmap， 我也可以得到它嗎？

高階主管

很有可能，你在招聘面試過程中已經會見了許多高階主管，但你必須再次見到他們所有人。你的第一關最好是“你老闆的同事”，這可能會是”執行長直屬 ”(the CEO’s direct reports)。如果不是，請將他作為你的第二關中；如果公司中沒有這個人，請直接將 CEO 作為你的第二關。與他們會面的目的是對你正在做的事情設定期望，以及他們什麼時候期望看到你的成效。這些會議應該相對簡短，因為你大多只是在他們面前露臉 (拜碼頭)。

要問的幾個關鍵問題：

- 在 90 天的試用期後，我將帶上 roadmap 進行審查，您會關注什麼重點？
- 根據其他新高階主管的成功和失敗，您有什麼建議嗎？
- 您能給我介紹一下董事會和其他高階主管的運作方式嗎？

董事會

在與董事會會面之前，你需要了解這些人。有些人通常會對董事會很熟悉，建議先認識他們，他們通常在法律部門，擁有“董事會處理者”的非正式頭銜，通常會是總法律顧問的行政助理， 你應該很快與他們交朋友。他們將能夠告訴您董事會成員有關各種個性的所有資訊，並協助您與他們聯繫。另外也可能要認識副總法律顧問，他們將能夠向你簡要介紹董事會內各個董事會成員的互動情況。你可能需要一段時間才能與董事會成員開會，但首先需要確定你將向哪個小組委員會報告（有些首席資訊安全官是向整個董事會通報情況，但大多是向稽核委員會報告）。你會想知道哪些董事會成員了解網路安全和技術，以及哪些人參與這些主題（這些可能不是完美的重疊）。看看你是否可以安排一些會議對這些議題感興趣的董事會成員的進行介紹。

未來要問董事們的一些話題：

- 您喜歡的其他公司的 CISO 向董事會報告的方式嗎？ 能向我介紹您的首席資訊安全官嗎？
- 至今圍繞網路安全的董事會對話中，缺少什麼？
- 至今的董事會報告中，您認為最有價值的是什麼？

TIP — 識別每位董事會成員參與的所有其他公司，並搜尋這些公司的網絡安全事件。在董事會成員參與的其中一家公司發生安全漏洞時，他們通常會對你的安全防護針對同類型的攻擊提出有針對性的問題。

瞭解你的環境

每次你聽到有關你的安全計劃的聲明時，你都需要詢問哪些系統在範圍內。你需要瞭解每個人忽視的差距 (或 out of scope) 在哪裡，因為他們只會考慮自己負責的資產風險。你將開始用探照燈探測 IT 陰暗面，尤其是當你注意某些系統安全漏洞未得到良好支援時。

GOAL — 了解你的安全計劃範圍。

不可接受的損失

你可能會想要一開始就直接就進入資產尋找問題，但你最好先瞭解公司最擔心的危害。你可以試著問每個利害關係人這些問題「我們公司最糟糕的一天對你來說是什麼樣子的？什麼會讓它成為最糟糕的一天？」，思考有誰依賴你和使用你的產品和服務也是個方向，想想你的公司會如何造成他們的傷害（希望是無意中）。這些通常就是不可接受的損失。

> 範例 — 在航空業中，資產可能包括飛機、 系統和登機報到櫃台。不可接受的損失有可能圍繞著對乘客的傷害。雖然這種傷害的原因可能來自資產（飛機墜毀、系統暴露敏感資訊、登機口導航錯誤導致錯過航班），但當你只看資產時，這些原因常難以察覺。

在公司環境中，重大影響（Material impact）通常就是不可接受的損失的定義：當發生重大影響必須公告在美國證券交易委員會來告訴您的投資者（如果您是一家美國的上市公司）。除了監管披露（來自各種隱私法）外，導致當成本超過一定閾值時，財務損失也可能會觸發披露。首席財務官 （CFO） 通常可以就重要性為您提供指導，有時會與總法律顧問一起討論這個問題。

此外，不可接受的損失通常也會隱含說明環境中的重要資產：如果攻擊者獲得了這些資產的存取或操作許可，將允許攻擊者輕易觸發對公司來說不可接受的損失。

系統類

最好用的資產管理工具是電子表格，不是計算系統數量，而是計算系統類型的數量的那種——你的公司可能有一個或多個資產管理系統來追蹤特定系統。在既有的電子表格中，你不僅要確認以列出已追蹤的資產類別（筆記型電腦、伺服器、路由器等），還要確認庫存管理中是否有漏追蹤以下建議的這些類型的系統，並將這些類別添加到電子表格中。

清單需要追蹤的系統類型建議清單

ENTERPRISE（支援員工和公司的實體）

筆記型電腦、桌上型電腦、虛擬機、伺服器（並確認 Windows 是否與 Linux 分開）、Active Directory domain、路由基礎設施、IOT（房間行事曆、監視攝影機、識別證讀取器、電梯控制器、冷暖空調、白雜訊發生器）。另請參閱後續的 Cloud 類和 SaaS 類單元。

PRODUCTION （如果您有銷售的產品）

開發實驗室、QA、構建系統、SDLC　基礎設施、生產環境伺服器、資料庫。此外，程式碼簽章基礎設施與自動更新也可能是相關的類別。另請參閱後續的　Cloud 類單元。

DATA CENTERS（如果您管理任何資料中心）

CLOUD

“多雲”通常意味著每個開發單位自由選擇其使用的雲服務提供者。通常，你可能會發現，即使是同一雲供應商中的系統也在分給許多獨立的管理者帳戶進行管理 – 獲取完整清單的最簡單方法可能是與財務中的應付賬款團隊聯繫，以確定雲支出的實際狀況。

INTERNET GLUE

您可能有自己的自治系統（Autonomous system, AS ）用於管理路由。您可能有 DNS 網域。確定誰追蹤和管理這些系統（並瞭解可能在外部管理系統的位置），例如在各大洲天高皇帝遠進行行銷的微型網站是一個不錯的檢查對象。

數據資料類

雖然大多數人直覺認為系統是重要資產，但其實對於大多數企業來說，數據資料才是你的重中之重，皇冠上的寶石，你最重要的資產。在傳統的非雲環境中，通常可以從大型存儲集群的系統來查找大型資料儲存。但現在並非所有數據都儲存在海量儲存集群中，而是存在雲中，數據資料經常可能出現在令人驚訝的地方。有一些數據資料可能依法必須受到監管，而有些數據資料可能是業務上的敏感資訊不應外洩。瞭解你的數據資料外洩可能性是保護數據資料的關鍵。

你必須了解你的公司保留了哪些數據資料，以及這些數據資料的儲存位置。可能一些數據資料位於你管理的儲存中，一些位於 SaaS 應用程式，甚至第三方服務可能持有更多數據資料。雖然大多數組織都牢記著，最終使用者（end user）的數據資料很重要，但也不要忘記評估你的員工資料、還沒有合約關係的客人的資訊以及你可能從第三方獲得的任何數據資料。

應用程式類

雖然有時候會將系統與在其上運行的應用程式相混淆，但將應用程式本身視為也需要保護的資產會很有用。通常，應用程式的管理者與其運行的系統是不同管理者，且應用程式安全性通常與系統安全性有很大不同。瞭解公司有哪些應用程式對你的業務至關重要，尤其是在你嘗試進行合規時 ：例如，PCI 和 SOX 都需要公司識別特定的關鍵應用程式的類型。

SaaS 類

現代公司的重要業務已逐漸轉向使用軟體即服務（SaaS）。十年前，大多數 SaaS 應用程式都是 IT 用於後台應用程式的獨立服務，而現在 SaaS 生態系統遍地開花。公司授權業務單位採用 SaaS 應用程式，從研發、行銷、銷售到人資，建立了 SaaS 應用程式、資料流、身份識別與第三方服務整合組成的複雜網路生態。

你必須瞭解你的 SaaS 網格(SaaS Mesh)。以下是你要確認的項目：確定你的公司所依存的眾多 SaaS 供應商是誰（它可能比任何人想像的都要大得多）、識別哪些配置使用 SSO、找到有權存取你業務關鍵 SaaS 數據的第三方服務、了解取消流程、了解有哪些使用者具有重新配置關鍵 SaaS 應用的管理權限。

瞭解公司業務

希望你從事的是提供某種形式的商品或服務營利（或非營利）的公司組織。瞭解公司業務價值鏈對於你的成功至關重要。一方面，能夠使用與公司業務類似的語言來描述安全專案將有助於視為業務推動者。另一方面，不同類型的商業模式具有非常不同的安全問題，你應該優先考慮這些問題。

你不僅要了解公司業務的交易部分（如何使用金錢用來換取商品/服務），更要通盤了解通往這個目的的整個業務流程——甚至更遠。這可能包括客戶開發、產品開發、供應鏈管理、服務交付、客戶支援和許多其他業務功能。查看公司組織圖，並詢問每個部分如何對公司的客戶產生價值，可能會梳理出您不知道但仍然需要保護的業務流程。

GOAL — 學習你的業務的獨特元素以及賺錢的方式。
掌握業務用語，以便能更好地與利害關係人溝通。

假使每個公司都只有一個核心的企業 IT 功能，而且不同的公司的資訊安全需求看起來也相似（每個公司都需要維持最終用戶系統保持最新！），其他公司與你的業務模式還是會有相當程度差異的產品安全需求。在基於資產的管理方式通常會將重要資訊（皇冠上的寶石！）和關鍵系統標示為業務流程中的關鍵元素。

物件租任業

主要行業：醫療保健業、教育業、住宿業、房地產

你的公司可能有長期的、半獨立的出租對象，他們會與你的業務模式糾纏在一起。他們與你就是傳統的房東/租客關係，公司的第三方、承包商甚至客戶對於公司的租戶也會是相同方式運作。像是：大學裡的學生和講師、醫院與醫生、長期獨立顧問之類的關係。你不一定有權向他們發號施令，他們可能有自己的IT系統不受你管理，但你仍必須支援它們並將其整合到你的系統中。雖然你可能利用身份識別和身份驗證作為施力點來要求他們，但您通常必須施加的更多影響力才能達到你的目標。

生產製造業

主要行業：製造業、汽車業、民生消費用品業 (CPG)

你的公司生產實物商品。你的IT安全計劃可能與公司的產品支援IT糾纏在一起，維護產品資訊安全將嵌入到公司資訊安全中。您最大的風險之一可能圍繞在產品設計相關，特別是外包的生產製造單位。

你的公司的供應鏈管理可能側重於供應商和貨運的安全和彈性。但談論「供應鏈」的資訊安全廠商一般都把重點放在軟體供應鏈上，所以當人們重複使用相同的用字時，要有混淆的心理準備。此外，有一些實物商品可能會有自己的IT（以及資訊安全）挑戰。

例如物聯網（IoT）可能是你需要關注的一個巨大領域，工業控制系統領域（ICS）也是如此。確保你的企業設施和製造系統之間的介面安全，尤其是針對勒索軟體的防護，可能需要你持續的高度關注。

軟體開發

主要行業：軟體業、SaaS 服務供應商、高科技產業

也許你的公司生產的不是實物商品，而是軟體。你可以將軟體作為銷售的服務（SaaS）來運營，也可以分發該軟體。這兩種銷售模型對於除錯和軟體更新有完全不同的運作方式；你也可能有差異甚大的威脅模型。對你來說，軟體供應鏈的重點是從第三方引入的軟體的血統和出處，主要關注重點在漏洞管理，但也需要關注完整性，確保攻擊者不會將惡意程式碼添加到你的軟體中。

如果打包軟體後分別以銷售或授權的方式售出，在客戶部署後如何修復缺陷（安全性或其他缺陷）會受到不同的限制。由於你無法控制客戶運行軟體的系統，因此你需要瞭解更新是如何進行的。無論是否提供自動更新基礎建設，都需要確保提供客戶更新檔案的完整性。在自動更新系統中，如何控制更新 、檢測佇列中的錯誤以及提供快速回應變得更加重要。

產品安全是您需要關注的一門學科 – 因為您的企業正在建立複雜的系統，所以軟體架構層級的安全分析並不能簡單地透過應用 IT 安全基礎知識來建立。如果您的企業強制執行軟體許可證制度（例如開源軟體），還請了解許可系統的運作原理，以及如何向客戶引入重要的軟體相依關係。你的客戶如何使用你的軟體將影響你更新軟體的方式（從而影響你自己的修補管理程式）。現代整個軟體供應鏈都會關注你的某些安全問題，因此令人驚訝的是，你最大的挑戰之一也可能是供應商管理。

軟體平臺

主要行業：SaaS、CSP

如果你可以操作自己開發的軟體，缺陷修復通常是一個簡單的問題，但客戶之間的隔離成為產品安全團隊的首要任務。您可能還必須處理員工如何存取客戶數據資料與操作環境的問題。客戶服務團隊通常只會因為客戶要求才存取客戶網站，但權限過大的存取權限可能會給企業帶來觀感不佳的風險。

假若維持網站可靠性工程（SRE）是你的公司最關注的焦點，跨租戶產生的漏洞大概就會是你最頭疼的問題，因為許多平臺公司將可用性作為運營 /DevOps/SRE 的重點，而不是資訊安全重點。緊隨其後的問題大概會是公司的服務是程式碼和客戶配置組合產生的功能，問題在於有時候如果不讓所有客戶都同意，某些功能的漏洞可能很難修復。

私生活領域

主要行業：金融服務、醫療保健、教育、政府、社交媒體

你所在的行業可能專注於提供個人化和量身定製的服務，作為服務的一部分，你將會與客戶的個人資訊（PII）糾纏不清。你可能會因為某些商業模式而有某些特別的資安危機，但如何保護客戶的核心紀錄—以及你如何利用這些紀錄—通常就是你制定安全計劃的主要重點。隱私是你的一個重大議題，你必須了解不管是你持有這些個人資訊，或是與其他企業合作，都將不斷地要求你改進個人資訊和資訊安全的保護措施。你的企業將不得不特別留意一下（或一千下）世界各地的監管合規要求，此外你可能還有其他認證要求要滿足。

如何共享並隔離你的客戶記錄是一個常見的挑戰，尤其是當你的公司使用者需要向客戶發送電子郵件時。如果一些客戶資訊是手動將應用程式資料寫入電子郵件，是一種極度高風險的操作，很容易被任何使用者介面缺陷與人為失誤觸發。

零售業

主要行業：零售業

如果你的公司直接在網路上或商店中向最終使用者銷售商品，你可能還必須注意偽冒欺詐和盜竊，無論是哪種公司，你會發現公司在很多地方重複收集資料，因此怎麼保護成了重點。在實體店面，你與實體安全團隊的關係更為重要。如何支援銷售設備變得重要—包括支付處理終端(如刷卡機)和結帳設備(如收銀機)。

此外，你的員工可能是大多是臨時工或兼差打工，通常只允許最低限度的連接到你的 IT 環境。你會發現持續強化培訓你的員工是很困難的，在你的業務流程中實施職責分離和稽核以檢測惡意行為者將是計劃成功的關鍵。

虛線業務(子公司)

主要行業：任何

你的公司可能擁有高度獨立的方式經營的子公司。雖然母子公司之間可能共享一個品牌，但 IT 系統常是獨立的。而你可能會有同行或接近同行的 CISO。 跨公司的資料存取可能是一個重要的挑戰，使用公司範圍內預算得到最大效果也是。

您的目標通常應該有三：
清楚地闡明整個公司的共同策略願景；
實現政策、架構和指標的標準化，讓每個人都專注於相同的措施；
並找出可以合理交集的地方將讓大家資源集中在安全產品上。

安全狀態

如果你瞭解你的環境，則可以針對可能遇到的攻擊評估其相關的安全控制措施。你的環境可能非常複雜，你需要從多個角度來分析，然後才能找到隱藏的缺陷。接下來的幾個小節會幫助你瞭解這些角度：你面臨攻擊風險來源、你已經擁有的供應商和解決方案、你的公司中資訊安全的機能，以及你需要的功能。然後準備好要開始進行的更改。

TIP — 建議你將安全計劃套用到 Sounil Yu 的《Cyber Defense Matrix》上。它與NIST（美國國家標準與技術研究院）網絡安全框架相當相類似且更好操作，這在利害關係人希望看到你的計劃與 NIST CSF 相對應的時，也很容易轉換。

識別攻擊

隨著你對環境的了解越來越多，你應該評估它對攻擊（從常見到深奧）的應對彈性。你應該了解常見的、眾所周知的攻擊類型（例如勒索軟體、網路釣魚、變臉詐騙、帳戶接管、DdoS 等）可能會在您的環境中運行。此外，你必須了解自己的服務如何導致你的客戶受到攻擊，以及在你為客戶提供的預設值選項下，有多少是可能被惡用的，哪些可能需要軟體缺陷才能暴露。

在你開始了解狀況時，請確認是否最近發生了一些攻擊並影響了公司。詢問過去事件，並瞭解公司對這些事件的反應。

GOAL — 以清晰而通俗的語言表達業務風險，以便與所有利害關係人進行溝通。

常見攻擊

為每個常見攻擊構建攻擊的路徑描述。在這個階段使用通用一般化的敘述方式，而不是過多的技術名詞。請忽略你當前的控制項，主要用於簡單地向合作夥伴描述攻擊。這些描述的一個重要關鍵是，你有辦法將攻擊分解為攻擊路徑上的多個步驟，接著你要評估安全控制措施，看看它們是否能在各階段減輕了危險。或者其中一些敘述可以組合成更大的攻擊，例如攻擊者可能會使用網路釣魚進行帳戶接管，然後開始使用勒索軟體進行勒索。

這裡有一些敘述可以說明你入門。

TIP — 保持敘述基本和簡單。它們主要用作警示，而不是對每個缺陷進行詳盡分析。與擁有完美描述相比，能輕鬆的溝通更為重要。

勒索軟體 — 攻擊者嘗試在機器上以任何可行的方法（網路釣魚、帳戶接管）。使用惡意軟體，該惡意軟體將利用該系統上任何可用的憑證（或利用已知漏洞），進行橫向移動、在我們的環境中傳播和竊取任何它找到的數據，刪除原始的資料。同時留下一個加密的副本。攻擊者可能以解密金鑰會向我們勒索恢復資料。

危害：能夠運行惡意軟體、允許橫向移動的管理憑證、系統上未修補的漏洞、缺乏資料備份/還原策略

網路釣魚 — 攻擊者向員工發送一條訊息，該訊息聲稱是來自公司或受信任的第三方的合法指示。

攻擊者通常試圖讓員工執行以下三件事之一：
打開有漏洞或可攻擊的附件/連結
直接在系統上安裝惡意軟體、
要求開啟某個網站並輸入其身份驗證。

危害：向員工發送惡意訊息的能力、員工與電子郵件互動的要求、安裝惡意軟體的能力、未修補的用戶端應用程式、可重複使用的身份驗證憑證。

帳戶接管 — 合法使用者將登入憑證洩漏給攻擊者，可能是其他來源的資料外洩（如重複使用的密碼）、代理攻擊（通過網路釣魚），或變臉詐騙。然後，攻擊者使用登入憑證登入帳戶進行惡意活動（例如以管理員身份安裝惡意軟體，在存儲的信用卡上購買禮物卡，收集情報以進行身份欺詐）。

危害：使用可重用密鑰（密碼、PIN）的身份驗證，缺乏活動監控來檢測偽冒欺詐/可疑登入事件

分散式拒絕服務（DDOS）— 能夠生成大量互聯網流量的攻擊者會發送該流量。在面向互聯網的關鍵系統中。該流量可能會使你的網路容量不堪重負，或者可能需要昂貴的應用程式處理才能處理。 導致你的關鍵應用程式無法正常提供服務。

危害：容量不足，無法將合法流量優先於攻擊流量

變臉詐騙（BEC）— BEC 與網路釣魚相似，因為它也是以向使用者發送初始消息開始，儘管該消息也可能是簡訊或電話。對手通常偽裝成高階管理者或合作夥伴，並要求目標員工啟動業務流程，例如轉移資金。

危害：未經身份驗證/容易欺騙的電子郵件，業務流程沒有申請/審核機制

針對行業的攻擊

現在，你已經考慮了任何公司都可能遭受的常見攻擊，請接著考慮是否存在與你的行業相關的具體的攻擊方式。也許是常見攻擊路徑的衍生手法（例如，當針對客戶服務的員工時，帳戶接管可用於實施更強力的攻擊）。你必須處理這些你和你的競爭對手都需要擔心的攻擊。

一些可能有助於梳理這些問題的提示：

- 你依賴哪些特定的第三方提供關鍵服務？
  如果這些關鍵服務受到損害，這不僅會影響你的業務，還會影響你的客戶？
- 整個行業是否都依賴你和你的競爭對手作為服務提供者？攻擊者如何利用傷害你來傷害你的客戶？
- 如果你的一個員工完全耍流氓，不關心自己的下場，他們怎麼能濫用自己的特權造成最大的傷害？他們可以存取哪些資訊，這些資訊如何賦予他們更大的特權？（請注意，你並不是試圖找出內部威脅；你需要更擔心攻擊者接管你員工的存取許可或系統）

針對公司的攻擊

最後，你需要開始瞭解針對於你的公司的特別攻擊可能給你帶來問題的各種方式。這些通常是以下的原因造成的：你可能使用或繼承了特定的設計或實作細節，並且通常不易被識別出來。從好的方面來想，公司裡會有人知道其中一部分，通常只需要問問就會知道。

一些可能有用的表徵：

- 我們的客戶應該使用哪些配置，但大多數卻都沒有？為什麼？
- 如果某人明天離開公司，誰會給我們造成最大的傷害？ 為什麼？是否他們維護的系統、流程與他們獨有的知識技能有關？
- 我們最脆弱的系統是什麼？
- 我們在哪裡擁有最多的技術債（先求有、苟且或便宜行事、或暫時妥協求未來有機會再來修復的部分）？

瞭解你的供應商

很有可能，你會有許多供應商為你的團隊提供安全服務或工具。而且，當你在LinkedIn上宣布了你上任了新職位，那麼更多的人將會嘗試與你接觸。在處理新供應商之前，你應該掌握現有供應商。

你的財務或採購通常可以提供一份清單，列出哪些供應商的採購項目已編入預算。在與他們交談時，你同時也要了解採購流程，如果你想快速取得技術或服務，你最該關注哪些圈子。在進行這些對話後，請確認現有供應商合約的續訂週期。對合約還有三年的供應商打交道，以及馬上就要進行緊急續約的供應商處理方式是截然不同的。對於正在進行的合約，請驗證是否正確估計未來幾年的續訂成本。

GOAL — 了解你目前已經涵蓋的安全需求，以及你的安全系統的限制是什麼。

整合/託管供應商

你可能有供應商提供安全管理解決方案，或者採購其他產品提供的加值安全服務。你要儘速與他們接洽，尤其是技術架構師、解決方案工程師或定期與你的公司互動的工程師。問他們與之前你問團隊相同的問題，了解他們正在為你解決哪些問題，以及他們認為你接下來應該解決哪些問題。向他們詢問你現有解決方案的成效。可以試著問問「如果我們停用某產品，我們甚至會發現嗎？」他們通常會幫助你找出哪些產品從未很好地整合過，並且可以納入你的安全計劃以瞭解下一步該怎麼做。

平臺

你的一些供應商也可能為你提供多種服務的大型平臺。向他們要求一些簡報（例如要求查看上一季的業務報告）或有助於你找出你曾向整合商提出的相同問題「停用某產品...」。但通常一個更有效的問題是“我們支付了什麼，但沒有使用？“ 雖然敏銳的供應商會擔心這是為了開始議價的起手式（而且通常是），不過利用你的前任CISO 沒有妥善使用的部分，常常可以殺價成功而取得一些勝利。但同時最好可能也要問一下其他人為什麼這些功能從未使用，以確保供應商不會低估整合的複雜度。

單點產品

在你的整個環境中，你也可能找到單純解決某個特定問題的單點解決方案。通常，問題發生的當下沒有其他選擇時就會安裝單點產品，但隨著時間的流逝，其他選擇可能會引起你的注意。查看單點解決方案的安裝時間，並查看這些系統是否仍在使用並為公司提供價值，或者它們是只是安裝之後被遺忘。也許你現在有一個新的平臺這包括此功能，或者可以升級到更新的版本。但在你的前 91 天，移除一個單點產品並不是你的首要任務，除非它造成了重大的業務摩擦、本身已經無效或對你的團隊有很高的維護成本。但是，一個同時滿足上述三個條件的單點解決方案可能是你正在尋找的初期快速制勝目標。

審計/顧問

你的安全計劃可能同時有審計員（審計，外部稽核，根據標準證明你的團隊或公司合規性的供應商）與顧問（在你的計劃中找到特定標準尚未達標的特定差距的供應商）。

你應該瞭解你的哪些供應商屬於哪個類別，因為你通常付錢給審計員目的是給你一個及格的分數（所以你的員工不會告訴他們問題出在哪裡），而你付錢給評鑑顧問是幫你找不及格的部分（所以你的員工喜歡告訴他們哪裡出了問題），你要盡可能的深入挖掘你的顧問的知識。

內部的

你也可以在內部嘗試自己構建安全服務和解決方案。你的團隊可能會向你指出已經有哪些自建的服務，你最好馬上就先瞭解它們是什麼，以及你的團隊如何維護這些服務。尤其是當你發現最後一個維護關鍵服務的人，才剛被你炒魷魚，將會無比的尷尬。

網路保險 / D&O

了解你的公司的網路保險戰略非常重要。不僅是誰承保它，還要知道它承保範圍，重要的是發生什麼狀況什麼可能讓你的公司可以向他提出支付保險金。當保險續約簽訂時，你的職責是什麼 —也許你會需要向保險業務員說明情況。

TIP — 檢查公司的董事及主管（D&O）保險。如果 CISO（即你）正在做薩班斯–奧克斯(沙賓法案)聲明，則堅持在D&O保單中也將你的名字列入。

評估你的安全計劃

到目前為止，你已經瞭解了公司的環境、面臨的風險以及安全計劃如何應對這些風險。現在你需要開始評估該計劃中的差距（gap）。評估出來的差距越具體越好；例如「安全性沒有被納入軟體開發生命週期」這樣的模糊發現，在溝通方面就不如「開發團隊 X、Y、Z 沒有將安全測試作為其品質保證計劃的一部分」有用。

找差距的一種方法是檢視現有的每一條控制聲明，例如（“我們平均在 7 天內修補關鍵漏洞”），提出問題以識別出該聲明中的差距：

- 這個度量指標包括哪些系統？
- 這些系統上的應用程式包括哪些（你如何得到漏洞資訊）？
- 如果平均值為七天，那麼離群值是什麼？有多少漏洞的處理時間超過兩倍的平均值？
- "關鍵"是如何定義的？有哪些重要的漏洞未被視為關鍵？
- 是否有例外？如何衡量？如果一個漏洞永遠不被修補將會如何影響該度量指標？

除了你自己對計劃的評估外，你還需要創建一種共用該評估的方法。通常，這是你在進行董事會報告時就已建立完成，現在，你也可以將它用在與利害關係人進行溝通。

GOAL — 了解你的安全計劃中的差距，並建立清晰的溝通方式來表達這些差距。

公司視角

當你評估你的計劃時，評估它的一個維度是公司視角：了解風險聚集的傾向，並將其與公司管理一般類別風險的所有團隊進行比較。有些團隊會與資產類別保持一致，例如你的公司風險管理團隊會同時處理 IT 團隊維護的系統相關的風險，也有團隊會拆解許多子團隊而個別會具有更實際的任務，例如安全教育團隊可能幾乎完全專注於培訓和品牌推廣活動。

企業 IT團隊

這個領域可能感覺是最千篇一律的，每家公司都會有相似的IT困境，但它通常是大多數攻擊路徑進行的地方。要確保你的安控機制正確的按他宣稱的方式工作（你選定的 MFA 可能非常好，但或許攻擊者找到未部署的系統來攻擊）。IT 們是否與隱藏的 IT們（在 IT 部門以外也支援的 IT 們，通常是各部門比較熟IT的人）保持良好關係？瞭解誰負責最終使用者資訊安全，以及最終使用者對該介面的感受，如果有問題，改善這些通常是一個唾手可得的改進成果。

合規團隊

大多數情況下，合規性會是產品管理要求，而不是安全要求。但大多數公司會將推動合規計畫的團隊視為安全團隊，把它當作產品需求來源來確保公司的安全。在公司對客戶銷售產品的評估階段以及後續階段，你有可能會需要向客戶宣稱你是產品經理，協助公司主要產品經理的安全工作。對於你向客戶銷售的所有產品，請務必瞭解你銷售對象的每個行業所需的法規和認證。你自身可能不是醫療保健提供者，但向他們銷售產品需要你遵守 HIPAA。向美國政府銷售產品需要 FedRAMP。能符合全世界的合規清單是很重要，但不要忘了其中的每一個安全需求都是一個產品功能，也是可能的賣點。找出哪些產品需要哪些安全需求，與產品團隊跟銷售團隊討論，並將尚未滿足的控制措施進行比較。

銷售支援團隊

許多安全團隊經常忽視的一個部分是他們與客戶互動的方式。 因為這可能只是合規活動的延伸，填寫或勾選令人麻木的制式表單與調查問卷只為了滿足第三方風險管理（TPRM）的要求。不過這也可能是一個次要的商機，產品如何能更好地傳達安全計畫。安全團隊還可能提供某種產品行銷。瞭解你的團隊在整個上市生命週期中所處的定位，以及你的利害關係人有誰跨足行銷和銷售。

產品安全和軟體開發生命週期（SDLC）團隊

產品安全，包括工程、運營和客戶支援，是你最需要仔細溝通的團隊。你的安全計畫的差距對於利害關係人來說通常不是要緊的問題，但是研發團隊是他們的金雞母。因此這會是你常找到風險並被延遲未修復的地方。找到戰友支持你的計畫，將作為快速獲勝的機會。

產品安全團隊通常直接隸屬於管理全公司的安全團隊之下(例如資安team隸屬於風險管理會之下)，制定良善的 SDLC 安全計畫可以在許多產品實體之間共用。SDLC 安全計畫通常包括軟體供應鏈的完整性（確保您的軟體不被竄改）、第三方軟體管理(追蹤和修復已知缺陷）以及保護內部開發的代碼（通常使用安全測試、開發人員的教育和程式碼混淆的方式進行）。

安全運營/事件應變團隊

當警報觸發時，通常會有某人進行應對。你需要確保這個人是公司中的成員，並了解他們如何處理警報和處理這則警報資訊。對於日常問題（例如，工具觸發的警報），你也要追蹤修補流程，查看營運團隊的營運模式是否與修復團隊的營運節奏相符，許多公司中的主要摩擦就是警報驅動的營運團隊試圖將修復工作轉移到基於專案的開發團隊中。

接著你必須了解針對重大事件和違規行為的回應計畫。確保你的事件回應計劃包括保留證據以及與通訊團隊(網路服務商)的整合。

瞭解你的公司如何從事件中吸取教訓。找出最近發生的幾起重大事件，並查看事件發生後的處理報告，以確定公司是否有吸取教訓。接著了解有哪些未解決的事件仍然懸而未決。

威脅情資團隊

瞭解你的團隊如何及時瞭解不斷變化的威脅形勢。可能是你三不五時看一下 Twitter 和LinkedIn。也或許你有一個更系統化的方法來瞭解攻擊者並調整你的安全計劃。並將這些資訊回饋到你的攻擊應變計畫中，使其保持最新狀態。

內部教育團隊

大多數公司在某種層面來說都設定其內部使用者作為安全的最後一道防線。雖然你的計畫應該把重點放在消除這種依賴上，讓使用者能更安全操作，不過你也需要了解你是否制定了正確的教育計畫，讓使用者受到攻擊的時候能產生警覺。

人力資源（HR）團隊

HR幾乎保存了所有的員工數據，但更重要的是，它們通常是公司中兩個最重要的安全流程的起點：入職和離職。在清理圍繞入職與離職過程的安全問題時，你通常會獲得一些快速的勝利，你同時也應該確保這些安全議題被解決：提供員工系統和身份驗證器、契約者（尤其是「被動離職」的人，他們的工作時間被降至零但工作合約未終止）、對 SaaS 應用程式的授權（和取消授權）、安全規範的培訓。

風險管控表

風險管控表並不是風險紙上談兵的地方，必須視為是一個可能實際產生但未發生的影響。如果你能分析每個風險管控表的副本，你通常可以找到一些你可能想知道的具體和尖銳的風險。對於任何處於活動狀態的風險管控表，你需要瞭解每個風險的消除標準，有可能各寫各的。瞭解需要什麼完成哪些管控才能從管控表中消除風險，這將使您能夠推動更多可操作的計劃。強制套用一致的成功標準（分析的方法論）作為風險管控的一部分也可以協助清理你的分析過程。

風險視角

評估安全計劃的另一種視角是通過風險的視角來看待計劃的任何部分。有滿多組廣泛使用的風險清單可選擇，這些風險幾乎跨越了大部分企業的安全計劃需要解決的每個部分。特定的技術實作可能使用於特定產品（例如雲安全態勢管理，CSPM 用於解決應用於雲服務提供者的錯誤配置），釐清這些領域將使你快速確認你擁有全面的強大安全計劃。通常，你需要一個能跨越多種風險的解決方案 ，例如一個完善的存取控制系統應該具有處理身份驗證和授權、應用程式暴露、橫向行動和流程管理不善的能力。

身份驗證和授權的風險

當使用者（或自動化處理流程）嘗試存取系統或功能時，這個身份驗證與授權將涵蓋了如何決定、是否允許他們這樣做。常見的重要元件有這些：通常是身份識別（Identity，實體是誰）、身份驗證/身份驗證（Authentication/AuthN，如何證明他們是誰）、授權/身份驗證（Authorization/AuthZ，檢查他們是否被允許執行操作）、權利管理（Entitlements Management，授予和刪除授權權利）。如果公司有使用單一登入（SSO）系統，該系統通常允許你集中管理身份識別、身份驗證和身份註銷，因此第一步是瞭解 SSO 的實作位置。某些時候需要整合外部服務時，你也需要評估外部服務如何管理身份簽章與介接。

接著查看你可能要確認的身份管理系統。人資部門手上持有員工身份的原始資料、外包或駐點的資訊可能由第三方管理，客戶資訊可能存在於另一個系統中。身份驗證通常是集中管理的，但是，與身份簽章一樣，有時候一些極端案例會帶來一些特別的挑戰。例如你需要為客戶資訊系統整合身份驗證，如果沒有整合，當客戶的員工轉換到另一個職位或其他公司時，你的提供給客戶的服務可能會有揮之不去的風險。

此外，許多公司在特例狀況進行授權時依賴手動、臨時的工作流程，例如使用服務單、手動稽核提權。配置和取消配置的自動化功能對於簡化使用者體驗非常重要，而基於角色的權限管理將減少因授予個別使用者過度的權限，而經常產生的混亂和風險。此外手動授權的瓶頸，可能會導致使用者出現原始授權規劃者未預見的用例建立合成身分。

TIP — 試著走一遍員工更改姓名的工作流程。不僅僅是更改顯示名稱，還包括更改帳號。處理不當的身份和權限的系統將給使用者帶來的困擾，將如同他被解僱並重新雇用為新員工一樣刪除帳號再重建，而不是讓現有的帳號接受這一變更。

配置錯誤的風險

你擁有的每個系統（無論是業務工具還是安全工具）都需要正確配置和維護。系統的預設值通常不能滿足你的安全需求，因此你需要能夠識別每個設定檔的缺陷並糾正它們。其複雜程度從非常簡單的設定（如單純的禁用功能）到相當複雜的設定（如不同元件之間作用）。端點、雲端和應用程式的各種安全設定檔管理系統都屬於這一類。

了解這個系統是檢測類（它只是告訴您存在問題）、預防類（不允許部署問題）還是反應控制類（問題自動修復），將對你的安全計劃是否能使用系統成功的處理錯誤配置至關重要。

應用曝光的風險

你的應用程式介面（Web、API 和用戶端軟體）通常存在巨大的風險，攻擊者可以在其中將惡意流量注入您的環境。盤點詳細的介面清單通常是保護它們的第一步 。

最常見的安全檢測控制措施是在請求或通信生效之前，監視惡意影響的控制措施，例如網路應用程式防火牆 (WAF)、欺詐檢測、電子郵件安全和端點防禦工具通常屬於這一類。此這個技術領域的安全控制技術可以是預防的或檢測。瞭解你的系統是拒絕流量，還是只在攻擊時發出警報，這一點很重要。同時，某些安全系統可能是分層的，由安全計劃的不同部分提供的類似功能，以確保你的公司的安全管控措施可以有效阻斷攻擊，又不會對檢測到的攻擊反應過度 。

了解你的應用程式安全控制是否有效是安全計畫的必要部分。驗證系統以防止錯誤配置降低應用程式介面的安全性是其中一個重要的組成部分；測試應用程式介面以發現缺陷是另一個重要部分。您想要找到快速修復的地方，同時設定能夠長期維持你的改進計畫。滲透測試、API 安全性和應用程式安全測試是你可以在制定計劃時參考的系統，不過實務上許多驗證系統是使用公司的自訂規則，來追蹤現有的控制措施。

橫向行動/惡意軟體的風險

當攻擊者獲得對環境的存取權限時，你的系統要有能力找出這個錯誤。也許在系統上留下了蛛絲馬跡，或者也許系統會注意到某些超出規範的行為。

這裡的功能應該集中在偵測成功的攻擊並防止攻擊擴大惡化。　許多安全計劃主要專注於在攻擊成功之前檢測和阻止攻擊；但也應該監視每個系統，以查找是否有攻擊繞過其他防禦措施並正在造成損害的證據。

安全計畫阻止常見攻擊媒介的能力越強，這些系統因常見的違規而產生的雜訊就越少，您就越能專注於檢測嚴重的違規。

TIP — 在評估你的橫向移動和惡意軟體能力時，對於每個系統都要考慮以下問題：“如果攻擊者入侵了這台機器，接下來他們會做什麼？滲透資料、修改資料、橫向移動？我們將如何檢測這些步驟？”

軟體漏洞的風險

如果你使用軟體，那它就會有漏洞。其中有些漏洞是你的軟體供應鏈中繼承而來的。有時風險來自檢測覆蓋範圍不足，像是你無法追蹤所有作業系統，應用程式和函式庫。此外也幾乎不可能完整識別所有你需要修復的漏洞。將你的程式碼與 CISA 已知漏洞目錄進行比較是確定漏洞修補優先順序的第一步。

非技術風險

除了上述技術風險外，還有一些與你的安全計劃相關的非技術風險，你應該留意。

知識流失風險

安全團隊經常可以取得大量資訊，追蹤這些資訊流向對於做出明智的風險選擇至關重要。資產管理是追蹤系統位置的核心，使用能追蹤控制的良好治理、風險和合規性（GRC）系統可能會讓您的學習曲線更平緩。 事件回應系統可以幫助追蹤你的系統性風險。 可以協助你了解你的安全計畫如何利用（或不利用）你的公司隨著時間的推移累積的知識，以及它的計畫成效。跨知識管理系統的資料分析可能是有趣見解的來源。

流程管理不善風險

如果沒有良好的流程管理，公司可能會難以維持現有的安全效益，新的缺陷會逐漸出現。 許多公司被動的依靠“人們做正確的事”，而不是透過健全的流程來建立良好的結果。 一些組織依靠專案經理來進行大多數流程管理，並透過各種知識和追蹤工具為他們提供支援。 使用好的流程管理系統通常在流程管理領域很有幫助，無論是漏洞修復還是事件回應。

你若打算推動自動化系統增強你的流程管理能力，公司有時可能會對完整的流程自動化猶豫不決，擔心自動化系統未偵測到初期或正在發生的故障時會出現混亂。 這時人類導入自動化運行火車的經驗在這裡可能有用：大多數火車幾乎完全由自動化驅動，而人類可以手動控制來停止火車（有時可以加速或減速）。 遵循一條自動化之路，讓人類擁有廣泛的控制權，同時允許大部分流程透過自動化運行，這是顯著提高效率的一個方式。

進行更改

確定你的改善措施

安全專案

你整理出了很多待辦事項在你面前。為了確定優先順序，你可以將你的待辦事項分為五類，從最差到最好依序是：某事你越做越糟，某事你無力可施，某事你能做的是少量的，某事你做得還可以，某事你做得很好。一個專案越能解決前兩個類別，你就越應將其視為優先事項。但同時你不應該好高騖遠一口氣解決所有問題，所以你應該優先考慮那些你做最少的事情獲得巨大進步的領域，而不是投入太多你尚不存在的政治資本，讓安安全專案進行昂貴而沒什麼成效的邊際改進。

快速取得成功

沒有人能在一家公司生存很長時間而不積累政治資本。即使有一個令人信服的事件促使公司雇用你，他們仍然希望看到你成功執行計畫。成功越多，你就越有機會成功。反之你失敗得越多，你就越教你的同僚如何讓你失敗。此類別旨在快速、輕鬆地獲勝； 通常是你的同僚在初次會議中建議你執行的項目。當你提出想法時，請根據其非破壞性（或積極破壞性）、可見性和有效性來確定其優先順序。 在開始第 90 天的簡報之前，先嘗試完成一些工作。在一些長期專案開始取得成果之前，你應該持續不斷地取得一些成果。

明顯的安全專案

很有可能，你是出於特定的原因被雇用，通常是為了解決每個人都看到的特定問題。這些將成為 前 12–24 個月安全計劃的支柱（如果這些問題真的很容易解決，那它們已經被解決了）。確保你有高階管理的支持者，並且明確將他們被納入你的計劃，讓他們在那裡支援你。

將所有項目都歸入這一類可能很誘人，但你真的不應該把你的團隊分散得太薄。對你能完成的事情要現實一點，然後在你提出計劃時再把它減半。如果你的估計過於保守，你可以做得更多；也總比你畫大餅做的比說還要少，對通常你來說是有害的。

長期變化

你可能還確定了要進行的一些結構性更改。要非常小心地宣傳這些專案，特別是當它們需要在全公司中進行戰略性變革時。弄清楚是否有快速獲勝或明顯的專案可以讓你開始進行，而不要在大家對你的執行力不了解之前推銷大型、破壞性的專案。

安全重構

治理

如果公司還沒有網路風險管理委員會，則你必需建立一個。這團隊會是你和你的主要利害關係人，也最好加入負責IT、工程、運營、人力資源、信任與安全、隱私、內部稽核和法律/合規的高階管理人。如果你對業務能有廣泛的監督，這可能是 C Level 高階主管，也可能是總監級別的同僚來扮演更具戰術性的角色。

網路風險管理委員會的任務主要是確保整個公司範圍內的網路風險保持一致。執行層面的戰術上講，這意味著在你向上介紹新專案之前，網路風險管理委員會應該已經瞭解這些專案，並同意這些風險是有道理的。

在某些公司中，網路風險管理委員會實際上會是兩個不同的團體。第一組是高階委員會，由高階管理人員組成，他們很少開會，也許每季度一次，主要作為董事會報告週期的一部分進行風險審查與資訊同步。你將向他們簡要介紹業務中正在發生的事情、風險狀況的變化，並可能在你計劃新的重大計劃時收集一些意見。第二組通常由來自這些職能部門的高級工作人員組成。例如你的直屬，以及直接負責每個功能區域的安全的董事/副總裁/架構師，該組協調實際發生的工作，並做出反應以調查新的風險領域或環境變化。

如果公司已經有一個執行長級別的風險管理委員會，你要將你建立的網路風險管理委員會與公司的風險委員會的工作委員會聯繫，而且你的成員通常會有很大的重疊。你要瞭解公司的風險管理委員會，並確保建立網路風險管理委員會以取得成功。

你的團隊

作為計劃施行的一部分，你很有可能需要調整團隊的配置。你有三個選擇：

- **你可以保持透明，讓你的團隊參與規劃。**你可能只參加你直接領導的團隊，也可能參加整個團隊與小組。如果你有很棒的人，但他們目前所做的工作不如你需要的那麼有效，那就做出這個選擇。你要讓他們參與決策，特別是如果他們的工作會發生變化，讓他們接受這些變化將是至關重要的。
- **你可以黑箱作業，並且大部分時間都在秘密地進行計劃。**然後，你要快速執行，讓那些不符合團隊發展方向的人離開，然後雇用新人。當你被帶進來就是為了取代現有的團隊改善現況時你就需要做這個選擇，也許他們的理念與其他高階管理人不符。但你應該進行謹慎，即使是你想留住的人也會對這種方法感到擔憂，導致比你預期還要多的人員流失。在這個模型中，通常無法如你預想的完成很多工作，特別是你需要花費大量時間招聘新人時。
- **你也可以和緩的調整。**通常是在公司中可以使用預算增加新角色，用來鼓勵現有團隊成員擔任這些角色。你可以讓你的員工知道團隊中的哪些職能將處於較低的優先順序（並且不會得到保證的報酬），這樣過大的團隊就可以更自然地通過調動或自願離職來減少。這種方法達到穩定狀態需要最長的時間，但破壞性最小。你可能仍然需要積極管理不適合你未來計畫的人，但你通常可以有更多的彈性來進行。

宣傳你的計劃

無論你的計劃在你腦海中多麼精彩，如果你沒有很好且正確的宣傳它，它就不會有效。宣傳不是一次性的活動。你可能會以為在簡報上進行展示並附有漂亮的投影片，然後就結束了。但相反的是，宣傳你的計劃是一個持續的過程，在你開始執行計畫之前就已經開始，並將一直持續到你離職的那一天。你需要以某種具體的方式分享你的計劃。你的目標應該有三個層次來宣傳關於你的計劃。在高層次上，討論你的框架。在中等級別，討論你的計劃。在詳細層面上，討論具體方案。

除了你正在宣傳的計劃之外，提出你的評估也是合理的，畢竟，正是你的職能來推動你的計劃，你可能需要讓你的利害關係人了解這些要點。雖然測量的數據有助於講述你的評估結果，但不要過度依賴數字。如果安全計劃僅通過指標即可輕鬆完成，那麼就不需要 CISO。

TIP — 你要在第一天就使用公司官方投影片模板。如果製作漂亮投影片有困難，請與行銷部的創意服務團隊中的設計師聯繫。投影片上的所有文字應至少使用 12 或 14 號字體，以確保易於閱讀。不要在投影片上使用大篇幅的文字，這是 Word 檔的用途。

框架

在你開始任何作業之前，你最好就擇定了一個框架了。你要有能力創建一個簡單的幻燈片來展示你的框架。它應該是一個乾淨簡單的模型，人們在與你見面後很容易記住。投影片可能會有三個支柱：維持穩定（保持現有的工作），現代化（替換無效或維護成本高昂的傳統解決方案）和優化（簡化流程和在可能的情況下實現自動化）。該框架要根據你在面試過程中聽到的利害關係人所要的點進行調整。如果他們問了很多問題，表示他們想更瞭解正在發生的事情，也許透明度也會成為你的核心支柱之一。

並非安全計劃中的所有內容都需要在核心框架中明確調用，你也不應該讓企業中的大部分人想知道它們在你的優先順序中的位置。

TIP — 有些人對於在描述新執行計劃時使用“pillars”這個詞產生非常負面的反應。你可以選擇使用 "focus areas"（焦點區域）或 "principles"（原則）來避免引起負面反應。

倡議的作用

對於框架中的每個支柱，你首先需要更深入地瞭解。你的倡議是主題支柱下項目集合群組。對於大多數利害關係人來說，這只是為了提供一個抽象級別。例如，在“現代化”這根支柱下，你可能有一個“將內部工具更新為當前最佳實踐”的計劃，該計劃將現有的機制轉換或轉移到你的團隊創建的工具，例如使用標準程式碼存儲庫、隨時更新過時的軟體庫。使用你的工具的其他公司團隊會對技術細節非常感興趣；而其他沒有相關的利害關係人通常完全不會理會你的這個倡議。

TIP — 使用引人注目的倡議名稱來推銷你的高優先級事項。例如，“消除安全障礙”是一個總括性的名稱，可用於處理任何你正在淘汰的無效流程；而“制止勒索軟體”可能是一個引人注目的倡議，能夠吸引大家參與一系列項目。

深入細節

雖然不是每個利害關係人都會關心你打算推動的每個專案，但每個專案都應該會有人需要瞭解它。對於計劃中的每個專案，你應該記錄一些事情。你會有一個簡單的描述(例如“將 SSO 轉換為 FIDO2-MFA”的專案可能會描述 「升級我們的單一登入，以便我們可以使用基於身份的驗證機制，同時不再使用密碼」），並解釋了為什麼會這樣重要（例如：“風險：當前的 SMS-Push 2FA 系統可能受到網路釣魚和 SMS spamming 攻擊 “），這是會你的計畫的里程碑之一。最重要的是，制定成功標準。例如（"所有使用 SSO 的系統都要支援新的 FIDO2 MFA 體系結構"），其中可能需要列出有明確的例外（"當前不使用 SSO 的系統不在此專案的範圍內"），當出現"所有"的關鍵字時就要明確地列出例外。

當一個專案變得備受矚目時，你要有一種簡單易行的方法來進行溝通，像這樣的簡單描述就成為你和你的利益相關者之間的合約。

取得支持

一旦你在計劃中寫入任何內容，你就要確定誰需要知道，並事先告訴他們，最好是已經與他們討論過。制定你的拜碼頭名單的一個簡單標準是：”如果這些人會因為不是從你的口中聽說要開始執行某個特定項目而感到驚訝，就應該加入名單“。事先溝通可以確保他們知曉並且不排斥即將發生的事情。你的工作目標很大一部分是消除任何意外，所以制訂這個名單並事先取得共識是很重要的。按清單拜碼頭時最好只是一個禮貌的溝通，因為他們已經事先向你瞭解了該項目，或者與你共同確定了對該項目的需求。

與利害關係人分享

現在是重要而有些可怕的部分：宣傳你的計劃。除非你的計劃目標是摧毀你的團隊，否則你應該都從你的團隊開始。你要向他們展示從草案到立案，以及你對利害關係人的承諾。你的團隊應該在第一個月內看到你的計劃的第一個草圖（即使它主要是試探性的）。

與同僚一起審查的草案你最好在第二個月開始之前準備好，你的目標是獲得同僚支持並就成功標準達成一致。如果你的計劃中有任何內容需要你的同僚同意，請確保在你開始向你們共同的其他同事展示之前，你已經與他們會面並得到了他們的同意。

在第 91 天（你就任三個月後），你必須準備好最終計劃。 將計畫向執行利害關係人傳達；但在進行任何形式的小組展示之前，你應該先與他們中的大多數人單獨分享。如果之後你需要向公司的執行團隊介紹你的計畫，最好大家都到齊再展示一次。雖然你之前都與他們個別私下都達成了一致，但確保他們在彼此面前達成一致對於你保持進步非常重要。

展望未來 91 天

恭喜你熬過了擔任 CISO 的頭 91 天。 希望你能將你就職之初的實務應用到你擔任 CISO 的時間；這不是一個能夠一勞永逸的過程。 你應該不斷了解你的環境，從利害關係人那裡獲取回饋，確定改進方法，並追蹤和衡量你的計劃的有效性。

為了簡潔起見，這篇文章跳過了許多你還需要注意的非常重要的工作，因此至少想給你留下一個關於《如何成為 CISO》未來文章中可能出現的內容的快速總結指南，希望你們都喜歡這本書。

- 指標、風險量化和風險條件（描述風險而不嘗試衡量風險）
- 向董事會彙報
- 人才發展
- 完美的演出
- 取得預算

如果你是專門處理雲的首席資訊安全官，那麼你很幸運！在由兩部分組成的指南系列（第一部分和第二部分）中提出了一些量身定製的建議。

其中大部分內容將是你在此處閱讀的內容，但有更多詳細資訊和具體概念供你考慮。

前 91 天清單

這是一個起點，可說明你確定應該完成哪些工作以及大致順序。如果你有辦公室主任、首席資訊安全官辦公室，甚至是行政助理或項目經理，請讓他們說明。

第 1 週

- [ ] 全公司面前舉辦全員會議進行自我介紹。
- [ ] 安排的團隊會議。
- [ ] 安排與同僚以及利害關係人的會議。
- [ ] 創建一個草圖框架來填寫你的計劃。

第 2 週

- [ ] 與你的同僚以及利害關係人會面。

第 3 週

- [ ] 與你的同僚以及利害關係人會面。
- [ ] 設定第一個快速成功計畫。

第 4 週

- [ ] 與你的同僚以及利害關係人會面。
- [ ] 宣傳第一個快速成功計畫並進行壓力測試。
- [ ] 安排第 13 週向高階管理層以及利害關係人進行簡報。

第 5 週

- [ ] 與你的團隊一起審查你的發現並起草計劃。
- [ ] 承諾你的第一個快速成功計畫。

第 6 週

- [ ] 定義未來 18 個月的戰略計劃。
- [ ] 執行你的第一個快速成功。

第 7 週

- [ ] 確定你將使用哪些基準來衡量你的計劃。

第 8 週

- [ ] 取得利害關係人對計劃中的支援 。
- [ ] 找到第二個快速計畫。 同時進行宣傳和壓力測試。

第 9 週

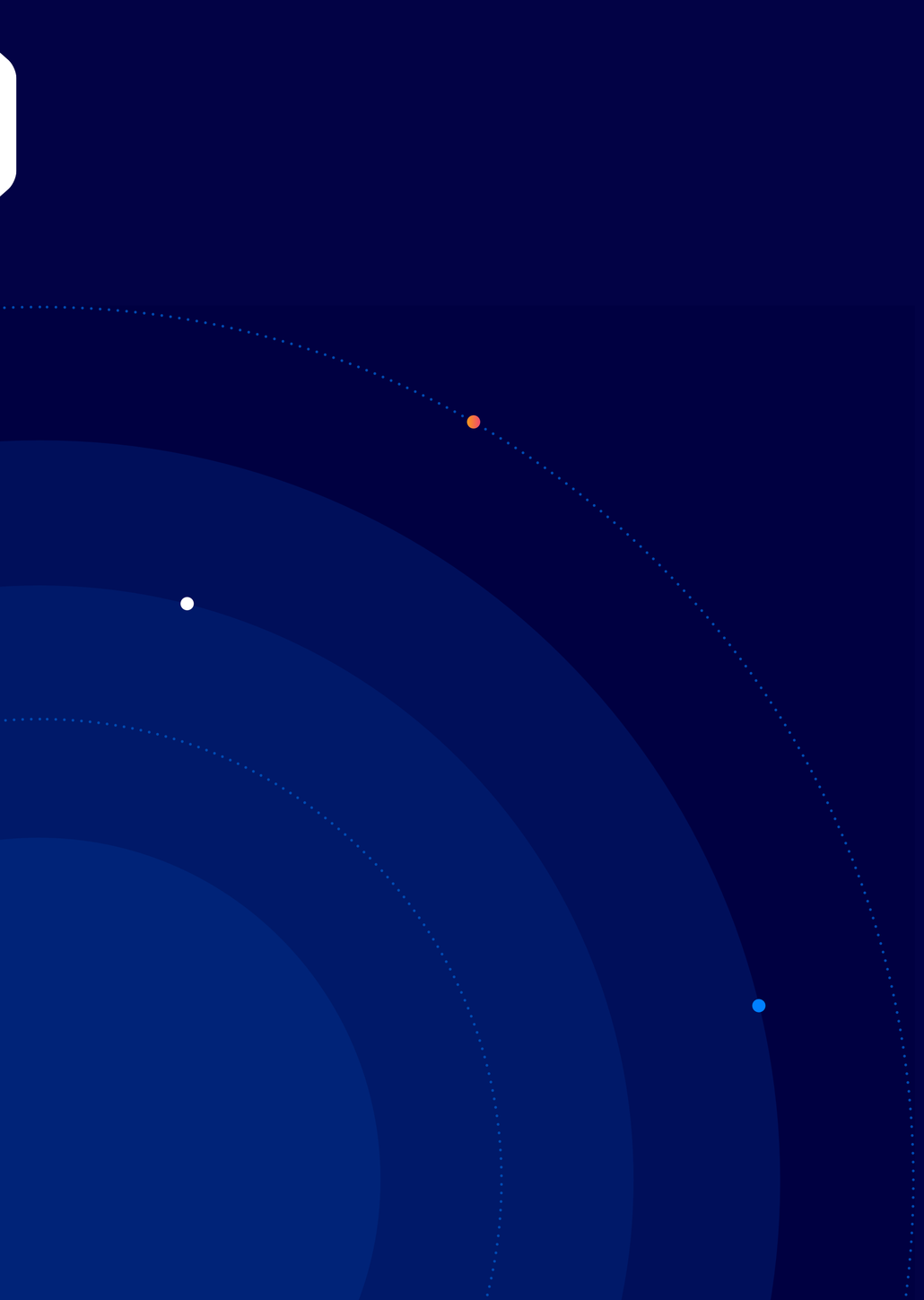
- [ ] 執行第二個快速成功計畫。

第 10 週

- [ ] 評估計劃找到的差距分析，準備選擇優先順序。

第 11 週

- [ ] 與各個高階利害關係人和他們直屬下屬進行宣傳計劃。



特別鳴謝

任何首席資訊安全官都不應該獨自學習如何自己完成工作，即使在撰寫關於如何成為首席資訊安全官的指南時也是如此。我從很多人那裡學到了東西，但我特別感謝少數有意或無意地幫助編寫本指南的人。不過內容有錯誤仍是我的鍋。按名字倒置的字母順序：克莉絲蒂娜·香農、大衛·斯派克、紀堯姆·羅斯、耶爾·納格勒、艾倫·奧爾福德、克爾斯滕·大衛斯和加里·海斯利普。